Cyber Security and *Habeas Data*: The Latin American Response to Information Security and Data Protection

Luisa Parraguez Kobek*
Erick Caldera**

ABSTRACT

Habeas Data is not a commonly known concept, yet it is widely acknowledged in certain circles that deal with information security and data protection. Though it has been around for decades, it has recently gained momentum in Latin America. It is the legal notion that protects any and all information pertaining to the individual, from personal to financial, giving them the power to decide how and where such data can be used. At the same time, most Latin American countries have created laws that protect individuals if their information is misused. This article examines the concept of *Habeas Data* from its inception to its current applications, and explains the different approaches and legislations passed in Latin American countries on data protection due to the rise of global cybercrime.

Keywords: *Habeas Data*, Latin America, data protection, cybersecurity.

* PhD. in International Relations from Universidad Nacional Autónoma de México and a Bachelor of Arts Degree in Political Science from McGill University in Canada. She was the Leading Researcher at the 2014 Yale Research Summer Program where this research began and is currently Professor and Researcher at Tecnológico de Monterrey, Mexico City Campus, luisa.parraguez@itesm.mx

** Senior Research Assistant at Tecnológico de Monterrey, Mexico City Campus, caldera.erick@outlook.com The authors greatly acknowledge the research assistance provided by Francisco Garcia and Ivan Morales for this paper.

Recibido: 1 de junio de 2016 / Modificado: 15 de junio de 2016 / Aceptado: 30 de junio de 2016

Para citar este artículo

Parraguez Kobek, L. y Caldera, E. (2016). Cyber Security and *Habeas Data*: The Latin American Response to Information Security and Data Protection. OASIS, 24, 109-128.

DOI: http://dx.doi.org/10.18601/16577558.n24.07

Ciberseguridad y *Habeas Data*: la respuesta latinoamericana a la seguridad informática y la protección de datos

RESUMEN

El *Habeas Data* no es un concepto comúnmente conocido, sin embargo, es muy destacado en ciertos círculos que tratan con la seguridad informática y la protección de datos. A pesar de que ha existido por décadas, recientemente se ha convertido en una herramienta de gran utilidad para las naciones de América Latina. Este concepto es una noción legal que protege cualquier tipo de información relacionada con el individuo, desde la personal hasta la financiera, dándole de esta manera a la persona el poder de decidir cómo y dónde se pueden utilizar estos datos. Al mismo tiempo, la mayoría de las naciones de América Latina crearon leyes que protegen a sus ciudadanos si su información es utilizada indebidamente. En este artículo se examina el concepto de *Habeas Data* desde sus inicios hasta su uso en la actualidad, se explican los diferentes enfoques que varios países de América Latina han adoptado y las legislaciones sobre protección de datos que han surgido debido a la ciberdelincuencia global.

Palabras clave*: Habeas Data*, América Latina, protección de información, ciberseguridad.

The right to privacy is to safeguard personal dignity… The protection of privacy is necessary for the legal order to guarantee respect for personal dignity.
Organization of American States (2016)

INTRODUCTION

The specialized agency of the United Nations for information and communications technology, the International Telecommunication Union (ITU), published in 2015 that 3.2 billion people were using the Internet around the world, 2 billion of which lived in developing countries; also that in 2000 there were 738 million mobile subscriptions worldwide and in 2015 there were 7 billion, with 69% of the population today being covered by 3G broadband (ITU, 2016). Most of the access through cellular phones is to social networking sites, while there is a marked rise in cybercrime. "Latin America and the Caribbean have the fastest growing Internet population in the world, with 147 million users in 2013 … only in Brazil, the cost of cybercrime reached 8 billion USD, followed by Mexico with 3 billion USD and Colombia with 464 million USD" (PwC, 2015). Global issues such as cyber threats and inadequate cybersecurity solutions can be viewed differently by countries with unequal levels of development, priorities and challenges.

Globalization has integrated political, economic and social systems together, which have grown with the emergence of the Internet and other online activities through the use of communication technologies. The increase

of such activities has caused concern in recent years due to the expansion of cybercrime around the world. The rise in Internet use, however, brings some uneasiness on "data retention, the increasing trend towards authentication of Information and Communication Technology (ICT) users, the relationship between service providers and law enforcement" (Genderen, 2008). Due to the merging of communication technologies, this has become increasingly important because traditional procedures and laws are not current enough to deal with the rapid advancement in ICTs.

Cybercrime encompasses a multitude of activities, all of them happening online, from financial attacks to espionage, information and data breaches. More often than not, an individual's personal data is put at risk due to the massive amount of digital information that is available. The 1950 European Convention on Human Rights states that "it makes no difference for data users or data subjects whether data processing operations take place in one or several countries". Cybercrime is a transnational threat and in a globalized world that means governments and law enforcement agencies have to work in a coordinated effort in order to combat this escalating threat. Among such international collaboration, there must be limits involved when dealing with an individual's personal information. In such cases, governments must guarantee that none of the fundamental rights held by individuals are being sidestepped for the sake of the investigation. Thus the importance of protecting individual rights through the writ of *Habeas Data*.

HABEAS DATA IN THE POSTMODERN COMMUNICATIONS ERA

Privacy must be given the utmost importance in a world that is transitioning from analog to digital even when information is readily available and easily accessible. As early as in the 19th century, Samuel D. Warren and Louis D. Brandeis published an article in the Harvard Law Review which stated that "privacy is a dynamic concept that can be adapted to the needs and values of individuals" (Warren & Brandeis, 1890). The same fundamental rights that were historically given to individuals must carry on in this new age of interconnectedness. Since the 1980s, the advancement in ICTs has grown exponentially to the point where individuals are now connected to the Internet at all times, hardly giving a second thought to the union of such technologies because people are used to being online through every facet of their daily lives. Due in part to the growing number of ICTs, two classifications must be considered: privacy of personal communications and privacy of personal data. These two concepts have become interrelated as communication and technology have become part of the globalization process.

Due to the openness of ICTs, a person's privacy is an imperative more so now than ever before. Searching for information is easier, and locating data has become a mere game of patience. Alan Westin's concept of privacy affirms that it is "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967). Cybercrime thus

becomes problematic for authorities because due to the sensitive nature of the information, authorities must treat the situation differently than they would a normal crime. Mechanisms that are well suited to the circumstances are required, while also respecting the rights of the person because "it is still necessary to guarantee the protection of fundamental privacy principles in national and international law" (Genderen, 2008). This notion is further complicated when the crime has been committed internationally, since each country has a different set of laws that might come into conflict with those in which the crime took place. Take for example how security breaches in Latin America are contrasting and stringent: some "countries require notification of a breach to the data protection authority within five days of its occurrence – not discovery" (Carson, 2013).

Cybercrime has been a severe problem around the world for many years, and in the last decade it has also deeply affected Latin American nations. It was not given priority until 1999, when the Organization of American States (OAS) established its first transnational cybercrime alliance. The objectives were: the cooperation among its members; to intensify technical and legal efforts; and to advise on the possible enactment of a cybercrime agreement and apply legislations aimed at combating this kind of crime. As a result, these efforts have allowed certain Latin American countries such as Argentina, Chile, Colombia, Costa Rica, the Dominican Republic, Mexico, Panama, Paraguay, and Peru to form part of the Council of Europe's Convention on Cybercrime[1] as Non-Members.

Updating the laws is one of the examples of the fight against cybercrime in the region, but a struggle of this magnitude is difficult to overcome without support. This is where the Council of Europe's Global Project on Cybercrime came into effect between 2009 and 2011. The main objective of this endeavor was to promote broad implementation of the 2001 Convention on Cybercrime through the implementation of:

> regulations and policies; financial inspections; data protection and privacy; preparation of prosecutors and judges; international cooperation with more than 120 countries; law enforcement; origination of regional parliamentary workshops in Latin America; and strengthening legislations in more than 100 countries (Laurant, 2010).

Despite international assistance, Latin American nations are still plagued by challenges that make cybercrime prevalent in the region. One of the main obstacles is that each country has a different perspective on how to deal with this threat, making it difficult to combat due to the lack of harmonization of the different laws. National legislations at the moment are not sufficient to deal with the character of crimes, which also means that investigations cannot be thorough enough

[1] The Council of Europe´s Convention on Cybercrime has as its main objective the pursuit of a common criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international co-operation.

because the law does not allow for search and seizure of intangible evidence such as data. At the same time, most of the region is lacking in specialized personnel and the equipment necessary to counter cyber threats. However, if the Cybercrime Convention is successfully applied to Latin America it would unify the current legislations with that of the other countries. This in turn would facilitate the cooperation between the different national and international enforcement agencies, while allowing for backing from both public and private entities.

EUROPEAN VS. THE UNITED STATES TRADITION

The issue with ICTs and transnational organized crime comes at a time when both the United States and Europe are regulating and combating illegal activities. The growth of ICTs, however, has made that difficult since enacted laws cannot deal with the speed at which regulations are so easily by-passed. Both the U.S. and Europe use state-centric as well as market based approaches, although such perspectives can have similarities they also have varying degrees of differences. These approaches arise "out of a growing awareness of the impact of globalization on scholarship and dissatisfaction with traditional models of public policy that fail to capture the shift in the relationship between public and private sectors in general" (Higgott, 2005). Although both employ these types of approaches, often when it comes to the state-centric approach, the United States places special importance on creating laws that govern the use of ICTs, valuing the idea of states being the ones that make up laws and legislation to protect not only their sovereignty and society, but also to show strength in view of new technologies that evolve faster than originally thought.

On the other hand, Europe has "created common standards, implemented through national institutions that countries take on board without feeling threatened by, or generating hostility towards" (Higgott, 2005). Europe thus demonstrates strength outwards by viewing the region as a whole and in such a way that it allows each country within its borders to adapt and transform. As a result, in today´s technological era what "looks like European weakness through traditional U.S. state-centric realist power politics lenses actually looks like strength through the newer lenses of the increasingly diffused and networked nature of power" (Higgott, 2005). By viewing states as companions, Europe incites cooperation rather than confrontation as in the case of the U.S.

Politics, however, is not the only force at work. The market provides a big push to the growing technological trend and ICTs are on the forefront of such technological leaps. As such, "political authority and powers are becoming increasingly dispersed while economic activities are getting more and more globalized" (Higgott, 2005). The rapid increase in the use of ICTs is partly due to the market demand of such technologies. This is a point that both the United States and Europe take into account when establishing regulations; yet, while the U.S. tends to legislate in conjunction with the global market, Europe has "developed sophisticated regu-

latory frameworks through its institutional architecture and the effective crystallization of international trade, investment and other common policies" (Higgott, 2005).

With ICTs growing at a rapid rate, cybersecurity firms especially from the U.S. and Europe, want to form part of the market in an up and coming region plagued by cyber threats. According to the Security Industry Association this would mean over half a billion dollars a year for security firms. The Latin American cybersecurity market is expected to grow from $5.29 billion in 2014 to $11.91 billion in 2019, at a compound annual growth rate (CAGR) of 17.6 percent for the period of 2014 to 2019 (MicroMarketMonitor, 2015). Mexico ranks as the second country with the largest number of cyber-attacks in Latin America, after Brazil. The constant increase in connectivity is one of the main factors that make cybercriminals direct their attacks against Mexico where cyber-attacks have grown 40 percent in 2014 (PwC, 2015). Cyber security companies like Symantec, Trend Micro and various other security firms promote their products in order to combat the rising threats that cyber-attacks pose to Latin America´s fledging communications infrastructure. This is an intermediary link between governments and the private sector collaborating to safeguard an individual's information.

Data protection in Latin America has been deeply influenced by the Council of Europe's 108th Convention on Data Protection. Latin American nations use the European directive as a model for creating regulations on the subject, which means that there is no overarching legislation that can be shared in the region to combat cybercrime; each country has its own legal framework that governs communications. Such regulations are lacking primarily because most, if not all, of the Latin American governments' communication systems have not had severe intrusions or attacks that would warrant a swifter response on the part of the government to modify its existing communications laws. However, it is important to note that although ICT laws in the region are not the most comprehensive, these laws are up to par with their European counter parts.

HABEAS DATA AS A LEGAL NOTION

Habeas Corpus is Latin for "you should have the body" and is the writ, or the formal written order and the legal notion used in Common Law systems to "bring a prisoner or other detainee (e.g. an institutionalized mental patient) before the court to determine if the person's imprisonment or detention is lawful" (Cornell University Law School, n.d.). Likewise, *Habeas Data*, translated as "you should have the data", is the writ, or the formal written order and the legal notion by which a person may request to see any and all information that a company or government agency has about them. The latter presupposes a guarantee about the manipulation and use of the information, and citizens or clients must have access to this information in order to verify, update or modify their information.

The right of *Habeas Data* can be traced to the first data protection law called the *Bundesdatenschutzgesetz* which was issued in Germany on October 7, 1970, and the Fair Credit Repor-

ting Act, which controls the collection, use and redistribution of any consumer information, and was issued that same year by the United States Congress. (Brigard & urrutia, 2013). In the 1980's the German Constitutional Tribunal defined *Habeas Data* as the "right to know what type of data is stored on manual and automatic databases about an individual" (Chirino Sanchez, 1997). Similarly, in 1981 the 108th Convention on Data Protection presided by the Council of Europe stated that the individual is given "a right to access their personal data held in an automated database" (Council of Europe, 1981). This concept was first implemented by various nations in Europe, such as Germany and Spain, which already had legislations that recognized the need to safeguard an individual's information from being misused. Eventually, more states within the European Union added data protection laws, such as Great Britain in 1984 and 1998, with the Data Protection Act[2]. All these efforts culminated in the 1995 ratification of the European Council's Directive on Data Protection[3].

There is no definitive description of "adequacy" because countries have different meanings of the term. For example, security adequacy is outlined by the European Commission with six principles: data quality and proportionality; security; access, rectification and opposition; transparency; purpose limitation; and restrictions on onward transfers. The security measures that each country in the European Union chooses to employ must in one way or another guarantee the safety and security of not just an individual's information, but also the data that pertains to a government's actions or of the people who reside within its boundaries.

The U.S. response to *Habeas Data* takes another approach, albeit one that contradicts the European system. In this case, governments have opted not to completely control and implement their own data protection laws, instead allowing for individuals to partially self-regulate their activities in regards to their own data protection. Moreover, it is observed that "although Americans are acutely sensitive about their privacy in cyberspace, they are also reluctant to empower the government to protect their privacy" (Kirsh, Phillips & McIntyre, 1996). Lately, this writ has been included as part of legislations and even some constitutions, particularly in Latin American countries, where it grants individuals the right to protect their information by issuing complaints. This allows for the individual to have a final say on the use and protection of their personal information.

With the world becoming more technologically adept, the danger of misusing data has become a serious concern towards the security and privacy of the individual. *Habeas Data* has become important in the creation of effective security measures and the involvement of the government in regulating data

[2] UK Data Protection Act of 1998: law that governs information security in the United Kingdom and allows for rights and liberties when it comes to personal data; it gives individuals the opportunity to maintain control of personal information.

[3] EU Directive on Data Protection: rules that regulate storage and protection of data in the European Union.

protection mechanisms, which are paramount if information is to be accessed, used or stored for safekeeping. This concern is a priority for most Latin American countries where *Habeas Data* is an integral part of a person's rights. Latin America may become one of the pioneers of the *Habeas Data* concept, which will become increasingly more relevant in the world, giving the region an important leadership position in the information security field.

Notwithstanding, there are differences between the constitutional provisions which provide for specific rights to privacy, *Habeas Data* and data protection. With regards to privacy: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks", according to the Universal Declaration of Human Rights (UDHR 1948, Article 12). *Habeas Data*, as discussed above, refers to the legal right of a citizen over his/her own information. Data protection denotes how the information should be obtained, processed and safe-guarded. Different countries in Latin America have various degrees of Constitutional Provisions and most have a provision for privacy, about half for *Habeas Data* and very few for data protection (see Table 1).

TABLE 1. CONSTITUTIONAL PROVISIONS WHICH EXPRESSLY PROVIDE FOR A RIGHT TO PRIVACY. HABEAS DATA AND/OR DATA PROTECTION

Country	Privacy	Habeas Data	Data Protection
Argentina	Yes art. 18	Yes art. 43	No
Brazil	Yes art. 5	Yes art. 5	No
Canada	Yes section 7 & 8	No	No
Chile	Yes art. 19	No	No
Colombia	Yes art. 15	Yes art. 15	No
Costa Rica	Yes art. 24	No	No
Cominic Republic	Yes art. 44	Yes art. 70	Yes art. 44
Ecuador	Yes art. 66	Yes art. 94	Yes art. 66
El Salvador	Yes art. 2	No	No
Guatemala	Yes art. 25	Yes art. 31	No
Mexico	Yes art. 6	Yes art. 16	Yes art. 16
Panama	Yes art. 29, 17, 37	Yes art. 44	No
Paraguay	Yes art. 30	Yes art. 135	No
Peru	Yes art. 2	Yes art. 200	Yes art. 2
United States	Yes 4th amendment	No	No
Uruguay	Yes art. 7	No	No
Venezuela	Yes art. 60	Yes art. 281	Yes art. 28

Source: Organization of American States (2012a).

COMMUNICATION AND INFORMATION TECHNOLOGY'S OVERWHELMING INFLUENCE ON *HABEAS DATA*

Individuals are more reliant on electronic communication now then they have ever been. In the past, sending a letter could take days, even weeks depending on where it was being sent. Nowadays, a person may send an e-mail, write a post on Facebook, a Tweet, post a Snapchat story for all to see, or a WhatsApp message to be read by one recipient or a group of people in milliseconds. That is how

far communication technology has advanced in our time, and it will continue to move forward in ways we have not yet imagined. Far more than the number of options available in terms of communication tools and social networks, it is people's reliance on electronic communications that makes information vulnerable. Individuals do not expect their correspondence to be seen by anyone but their intended audience, but that does not mean that it is not being monitored. In some cases, the government screens correspondence that gets sent from one place to another to ensure that it does not constitute a crime or infringe on national security matters. Other times, government surveillance can go wrong, thus incensing the very people it is trying to protect.

This is the downside to information technology: the more one tries to keep every piece of data secure, the more it can become an "ethical dilemma" (Dunn Cavelty, 2014). In an ideal world, individuals would not need to worry about their personal data and governments would not have to fear public discontent for keeping sensitive data secret. But this being a complex world, data can be used for the wrong reasons and can impact every level of society. A current example is the information released by Edward Snowden in 2013. The type of sensitive information that was unleashed angered many people, leading to strong criticism and in many parts of the world, an anti-American sentiment. It led to questioning the motives behind such an intrusion of privacy that involved world leaders and common people alike. Another more recent case would be the Panama Papers of 2016, which exposed 11.5 million leaked documents of financial and attorney-client information of a private Panamanian firm called Mossack Fonseca (Harding, 2016).

However, when it comes to information privacy "the reality is more complex, privacy and right to information laws act as complementary rights that promote individuals' rights to protect themselves and to promote government accountability" (Banisar, 2011). As such, privacy is constantly being contested by changing technologies and in response to those modifications "more than 60 countries have adopted comprehensive laws that give individuals some control over the collection and use of data by public and private bodies" (Banisar, 2011). Nonetheless, accessing data is becoming easier thanks to these new technologies, where a person can search for his or her own records without much trouble. International governing bodies and institutions are thus designing newer standards of data protection that are more detailed than ever before.

More countries have taken to the task of upgrading their privacy protection laws and a premier example of such inclusion within their constitutional rights is Latin America. Argentina, Brazil, Costa Rica, Paraguay, Peru, Uruguay are among those countries that have enacted data protection laws and made them part of the individual's human rights. This means that "approximately 185 million Latin Americans are covered by data protection laws" (Martínez-Herrera, 2011). Unfortunately, data security in this region of the world is often lacking because *Habeas Data* is still a novel idea. In addition, administering these

types of rules is particularly difficult in these countries due to: "1) limited budgets and limited regional experience in data protection enforcement; 2) a need for technical expertise in data security or privacy protection; 3) public distrust of government oversight and enforcement; 4) corruption issues; and 5) lack of public awareness of personal data rights" (Leiva, 2013).

LATIN AMERICAN DATA PROTECTION MANDATES

• Historical Conditions

During the 1970's Latin American leaders took it upon themselves to explore the possibilities of updating and strengthening the structures of information protection. At the same time, the authoritarian experience of the 1960's to the 1990's made it difficult for countries to incorporate openness. Keeping data secure is one of the main concerns of governments around the world. Still today, requesting sensitive government documents may meet the obstacle of national security interests of the State. Balancing privacy and national security has never been a simple task; trying to quell opposing opinions and maintaining interest in information protection has been challenging, especially when surveillance of the State into an individual's personal data is not tolerated by society. Critics tend to place special attention on the risks entailed by data processing. The historical background of the region, especially in countries where military dictatorships ruled with an iron fist, do little to help current leaders sway public opinion due to the years of distrust and abuse by the government.

• Impact of Society and Culture

Data protection has become a serious issue in modern society because accessing information is as simple as flipping on a switch. It is because of the inherent danger of such action that it is necessary to find a method to protect an individual's data from being abused. Instead, finding a secure way to manage and maintain a person's privacy intact, as stated by Manuel Martinez-Herrera:

> The individuals' have the right to control the information stored and disclosed about them. Such a right is, of course, paramount to protect an individual's image, honor and reputation as it is a way to try to control incorrect/inaccurate information that may damage such image, honor or reputation.

Society has taught the individual to be wary of intentions, as what may be veiled as something innocent can turn out to be criminal. Regrettably, this is also a culture in which it is assumed that whatever information or data being used, it will not be applied for its envisioned purpose. It is not a habit for the individual to ask how the information will be used or where it will end up. This overconfidence can become a problem in the long run. It is because of this very reason, that certain countries in Latin America are creating the tools for individuals to regulate themselves and have the final word regarding their information.

• Political Motivations

Politically, countries have had to adopt a series of laws aimed at better protecting privacy. It is imperative that governments guarantee that any and all data, personal or otherwise, not only be treated with respect, but also be protected from prying eyes. This has been a sensitive issue for Latin Americans since governments in the region have had a history of authoritarian rule and have been able to intrude at will if they deemed it necessary to protect national security interests. Because of this context, Latin Americans tend to lack the necessary trust in their leaders to allow for better equipped monitoring structures. Evidence of this is how corruption allegations in various Latin American countries tend to blow up into disproportionate scandals, regardless of the actual procedures specified in national laws. While the impeachment of a president may lead to them being found innocent, Brazilian public opinion has notoriously acted as if impeaching President Dilma Rousseff was either a veiled *coup d'état* or a farce created by the opposition. Even when pre-established procedures take place, society does not trust that they are serving their specified purpose.

There are variants of trust that a government needs so individuals can feel that their information will be respected. These include "political trust (political legitimacy), social trust (catalyzing effects of social capital) and technological trust (technological democratization)" (Blind, 2006). Most Latin Americans perceive a lack of those kinds of trust, because "a trusting person, group or institution will be freed from worry and the need to monitor the other party's behavior partially or entirely" (Levi & Stoker, 2000). The adoption of government regulations has been slow due to the skepticism that the governing body would put someone else's interests ahead of their own, thus "trust comes into play every time a new policy is announced" (Blind, 2006).

Countries in Latin America vary in the methods used to apply data protection. While some only have partial protection, others have a more advanced function within their respective societies. *Habeas Data* is constantly evolving, depending on the situation and the country's needs. A few countries in Latin America have moved forward on the progression of data protection (see Table 2).

• Economic Rationale

Information is more vulnerable during the transmission process when the data flows from one system to another, making e-commerce transactions and bank transfers especially susceptible to intrusion attacks. It is common knowledge that one of the most harmful ways of crippling an individual's and a government's well-being is by stripping them of their financial backing. Amongst the chief concerns in information protection, experts are creating new and innovative ways to guard against attacks of this nature. In certain situations, it "might become appealing for European… Latin and North American companies to open new subsidiaries or branches, outsource operations or use local…data centers" (Martínez-Herrera, 2011).

Security in the economic sense has to do more with the ability to guard one's data by

TABLE 2. DATA PROTECTION IN LATIN AMERICA: SELECTED COUNTRIES

Argentina	Argentina's version of *Habeas Data* is called "*amparo*", which is the combination of various other types of grievances that fall under the same provision. Provided under Article 43 of the Constitution, Argentina has one of the most comprehensive forms of data protection in Latin America. Imitating certain aspects of the Paraguayan form of *Habeas Data*, the Argentinian provision adds its own stipulations, including the idea of information privacy. The ratification of this law brought about the creation of the National Directorate for Data Protection, which is in charge of regulating, enforcing and securing data within the country.
Brazil	Brazil has a 1988 provision in its Constitution that spells out how *Habeas Data* can be used as a legal tool, thus allowing individuals to access, modify or correct information pertaining to themselves.
Colombia	Colombia adopted Law 1266 in 2008, with final action taken in October 2012 when the comprehensive data privacy Law 1581 was enacted. Similar to laws in Argentina and Uruguay, the new law prohibits transfer of data across borders to countries that do not have "adequate" data protection regimes as determined by the Colombian regulator, unless the data subject grants prior express consent. Secondary legislation, Decree 1377, was issued in June 2013.
Costa Rica	Costa Rica adopted a comprehensive data privacy law in September 2011. Among other requirements, in general, personal data cannot be processed without the express consent of the data subject.
Mexico	Mexico's *Habeas Data*, just like Argentina's, is also known as "*amparo*". Much like its Latin American counterparts and taking a similar approach as the European Union, Mexico has enacted data protection laws that are comparable in function to those of the other countries. These laws help protect information in such a way that they limit the compilation, transmission and dissemination of personal information. Analogous to the Argentinian case, the National Institute for Access to Information and Data Protection, also known as INAI in Spanish, is in charge of enforcing transparency and privacy laws. This falls under the scope of the National Law on Protection of Personal Data Held by Private Parties.
Paraguay	Paraguay enacted its data protection law in 1992, following Brazil's initiative, with slight modifications. It improved upon the foundations provided by the Brazilian law by offering the individual a means of accessing, changing, destroying, and ascertaining the aim for which the information will be used; a principle mentioned by Article 135 of the Paraguayan Constitution.
Peru	Peru mixes the data protection of both Paraguay and Brazil. On the one hand, it does not allow for the modification or correction of personal information stored in databases. On the other, inaccurate information cannot be disseminated, reproduced or moved from one database to another. It is different from the previous versions, as it only allows for one alteration of erroneous information. Enacted in 1995, this law can be found in Article 200 in the Peruvian Constitution.
Uruguay	Uruguay adopted an EU-style law in 2008 and received an adequacy determination from the EC on Aug. 21, 2012.

Source: Authors' compilation based on: *National Constitution of the Argentine Republic* (1994): http://pdba.georgetown.edu/Constitutions/Argentina/argen94_e.html; *Constitution of the Federative Republic of Brazil* (1988): http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html; *Mexico Federal Law on Protection of Personal Data held by Private Parties* (2010): http://inicio.ifai.org.mx/English/1%20Data%20Protection%20Law.pdf; *Constitution of the Republic of Paraguay* (1992): http://pdba.georgetown.edu/Constitutions/Paraguay/para1992.html; *Political Constitution of Peru* (1993): http://pdba.georgetown.edu/Constitutions/Peru/per93.html; Gutierrez & Korn (2013).

purchasing the adequate software required to protect against all manners of cyber-attacks, as "the economic considerations of security are more important than the technical considerations" (Schneier & Anderson, 2004). Although it is true that a variety of methods such as firewalls and e-mail encryption already exist to minimize the risks of any financial and information downfall; more often than not those same systems are not employed

"not because of the relative effectiveness of the technologies, but because of the economic pressures that drive companies to install them" (Schneier & Anderson, 2004).

LATIN AMERICAN ICT STANDARDS AND INFORMATION POLICIES

ICT standards show huge variation across Latin American countries. One key difference is whether the focus of the laws is the actual misuse of the information or its mere availability. When it comes to ICTs and data transmissions over the Internet, Argentina does not have specific rules concerning privacy. Instead, cases concerning violations to an individual's privacy are regarded the same way as if the offense occurred in outlets like the newspapers or television; where it is grouped with other online services such as "files, databases, or other technical media for data processing" (Cruz, 2012).

Colombia became the first Latin American country to adopt a comprehensive strategy of cyberdefense for international threats and cybersecurity for national threats in 2011 with the help of the Organization of American States. It established the national computer security incident response team called colCERT, the Joint Cyber Command (CCOC in Spanish), and the Police Cyber Center (CCP in Spanish). The country recorded fewer cyber incidents in 2012 than in 2011, pairing it with Chile as one of the few Latin American countries with that distinction (OAS & Trend Micro, 2013). Colombia's system concerning the transmission of data, utilizes more safeguards in that it "requires previous, express, and informed consent", but it is highly stringent on how personal information is processed electronically; Colombian law states that "personal data, except for public information, shall not be available on the Internet" (Cruz, 2012). The downside to this stipulation is that it does not take into account that the services provided on the Internet sometimes require personal information to sign up, and thus only treats the Internet as a communications tool.

The stage at which laws were created also affects their content, notably in whether older laws are adapted to the existence of the Internet or designed with the Internet in mind. Laws in Chile regarding information security and data protection have not been created *per se*, rather existing legislations have been extended to include certain characteristics specific to ICTs. Essentially, the processing of personal information is governed by the Law on the Protection of Private Life (n.º 19628) stating that "data processing that consists of personal information collection, processing, transfer and storage, and is applied to processing, collection and storage of data over the Internet" (Cruz, 2012). The international transmission of data is clustered into the notion of processing, which is allowed as long as the information being transmitted fulfills the directives found under the law.

Mexico's laws on data protection regarding the Internet are fairly new, considering that the laws were created at a time when it was already being used by a substantial percentage of the population. Provisions on international transfers receive the same measures of protection as would national use of data. Specified in Section 36 of the law on Personal

Data Protection states that "international data transfers are authorized as long as they are carried out in accordance to the privacy notice" (Cruz, 2012). The recent legislations on the subject mean that Mexican law is proficient enough to foresee scenarios that could come into conflict with privacy rights. At the same time, because they were designed with the Internet already in mind, the laws are flexible enough that they can easily adapt to the evolution of ICTs.

The mechanisms for information security that have been implemented in Latin America have not worked quite as well as hoped. Information systems can be effortlessly manipulated by unscrupulous third parties, while malicious use of personal data, proliferation of false bank accounts, dissemination of secretive government documents and fraudulent e-commerce transactions have intensified in the past couple of years. Criminal groups, hackers, and even whistleblowers have been able to bypass secure databases and obtain a treasure trove of personal and sensitive data. That data is more often than not used as bargaining chips when it comes to blackmail and corruption at all levels of society. The dissemination and distribution of personal and sensitive data is as much a business as it is a danger for all the parties involved, this is because "corporate malignity is the theory that business or entities ignore ethical standards and support malicious business practices" (Thomas, 2007). In some cases, leaked information stops moving in secrecy to turn up in public outlets, such as when in April 2016 the entire list of Mexican voters was found to be on sale in Amazon.com (García, 2016).

LATIN AMERICA'S OUTLOOK ON *HABEAS DATA*

The perspectives regarding information protection in Latin America are not optimistic. Most countries in the region lack the necessary mechanisms to prosecute those who misuse information and obsolete legal systems cannot compete with the advancement in technology and information services. Nevertheless, Latin America has the potential for improvement, grabbing one idea and adapting the borrowed model so that it can build better data securement methods and properly address the threats that have plagued the region. In the near future, Latin American nations may continue to emulate European data protection directives, modifying current laws and amending their constitutions even further to better guarantee the protection of an individual's data. Hopefully Latin American security measures can be enhanced with tools that are better suited to handle data in the region, and at the same time, give the individual better tools to protect themselves from their information being abused, whether it be by the government, organizations, agencies or other involved parties. Data security, as a basic right of every person in the region, should be assured protection regardless of the type of information that is stored.

The most likely scenario is that, although it has enacted various forms of data protection laws, Latin America, will continue to "protect" an individual's information without actually enforcing them. The measures in some laws are necessary, but are not ready to handle such a sophisticated set of circumstances, especially when the technological prowess of

the region is not up to par with that of more technologically advanced systems such as the United States and the European Union. Legal mechanisms try to contend with the rising demands of data usage, but the reality of most legal systems in Latin America is that they are not equipped to deal with the mounting complaints, partly due to the fact that information technologies advance much faster than legislations on the matter can be ratified.

Despite the difficulties related to legal systems that do not focus on implementation, the outlook for Latin American information security with regards to methods and the definition of how data exists in relation to governments and citizens, is a bright one. The right methods are being applied to a worldwide problem, solutions are being formulated, and in the end, the region is heading in the right direction. This initiative is but one stride on a long road of electronic reforms and data legislations. More is needed if Latin America hopes to strengthen its image in the international arena and become a serious contender in the field of data rights.

MODIFICATIONS TO THE CURRENT INFORMATION SYSTEM

• Public/private investment of secure data storage infrastructure

The progress on information technologies is rapidly increasing. If Latin America wants to be a pioneer of data rights in the digital world, it must first replace its aging equipment for newer and faster data processing units that comply not just with national, regional or even the European Union's directives, but with international protection of information practices. At the same time, the new infrastructure must effectively adapt to the changes in the way information is transmitted around the world. For this solution to take effect, there has to be a source of funding. It would be productive for governments to finance the operation in conjunction with private firms. The benefits of furthering research on the issue of data protection would benefit them both, which makes it a promising research opportunity for joint funding initiatives.

• Effectively sanctioning those who intrude in secure systems or propagate personal information

Governments should better enforce their laws regarding data, especially concerning legal sanctions for any and all involved in criminal activities that endanger information whether it be personal, public or governmental. Similarly, data should be better monitored, not necessarily to violate individual privacy, but to maintain order and to demonstrate to the individual that their information is being cared for. Updating relevant regulations and practices related to data protection would, in the long run, facilitate legal proceedings and bring about swift resolutions to security issues.

• Specialized agencies in charge of information transparency and data monitoring

Some countries like Mexico and Argentina have created governmental organizations

whose sole task is to protect information. Agencies such as these must, of course, keep the government accountable for its actions and provide information to any individual that requests a copy of their personal data. Latin American data protection agencies would have the expertise, tools, resources, and most importantly, the necessary training to deal with data intrusions. Having experts in this particular area can give people the confidence to place more of their trust on their government. Another option that can be explored is the possibility of forming a regional data protection center, which could be similar in function to the European Data Protection Supervisor[4], which ensures that government agencies and institutions follow correct data processing procedures and security policies.

CONCLUDING REMARKS

Globalization has brought about a world where Information and Communication Technology (ICT) connects most of the globe, obstacles are practically nonexistent and positive effect can easily be seen in day to day activities. However, as positive as globalization has been to society, it also has its downsides. The proliferation of cybercrime leads to the need for new frameworks to be designed in order to counter the rising challenges posed by the ICTs.

Latin American governments have gathered ideas on the regulations on data protection from the European information security model to suit the context faced by each country. Among the more notable ones are the inclusion of an individual's privacy as a fundamental right in various Latin American constitutions. The flexibility and adaptability of most Latin American laws on cybercrime provides an equilibrium between a person's privacy and the methods used to fight online crimes allowing for better protection of personal data in such a way that an individual's rights will not be infringed. Yet, there are still major obstacles that the region must overcome, especially in the areas of rule of law, trust and corruption where the regulations employed have clear areas of opportunity.

Although much still needs to be addressed before the Latin American region takes a lead in data protection, it is taking the necessary steps in the right direction. A joint effort among the Latin American nations would not only be mutually beneficial, but could also be advantageous at an international level. To achieve this goal, there are three areas of opportunity that must be addressed. Firstly, the need for collaboration between the government and the private sector is key; without either entity helping each other, research on the subject cannot be guaranteed to yield any favorable results. Secondly, strengthening sanctions and laws on cybercrimes is not enough to deter such offences from taking place; implementing legal sanctions to those who breach an individual's privacy

[4] The European Data Protection Supervisor is the independent institution within the European Council that has supervisory functions that certify that information is being protected and privacy is not being infringed upon. It also cooperates with other European agencies and consults on the development of new guidelines on data security.

is imperative for data protection regulations to be effective in the long run. Finally, homogenizing the region's data protection efforts into a comprehensive set of legislations would greatly increase the effectiveness of combating cybercrime and information breaches across Latin America.

REFERENCES

Anderson, R. & Moore, T. (2007). Information Security Economics – and Beyond. *Advances in Cryptology – CRYPTO 2007,* 4622, pp. 68-91. Retrieved from http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf

Anderson, B. & Schneier, B. (2004). Economics of Information Security. *IEEE Security & Privacy.* Retrieved from https://www.schneier.com/paper-economics.pdf

Banisar, D. (2011). *The Right to Information and Privacy: Balancing Rights and Managing Conflicts.* Retrieved from http://wbi.worldbank.org/wbi/Data/wbi/wbicms/files/drupal-acquia/wbi/Right%20to%20Information%20and%20Privacy.pdf

Barrientos, A. & Santibañez, C. (2009). New Forms of Social Assistance and the Evolution of Social Protection in Latin America. *Journal of Latin American Studies 41* (01), pp. 1-26

Bazan, V. (2011). Habeas Data in Comparative Law, with Particular Reference to the Bolivian Constitutional Reform. *Comparative Media Law Journal* (5). Retrieved from http://www.juridicas.unam.mx/publica/rev/comlawj/cont/5/arc/arc4.htm

Blind, P. K. (2006). Building Trust in Government in the Twenty-First Century: Review of Literature and Emerging Issues. *7th Global Forum on Reinventing Government*. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN025062.pdf

Brigard & Urrutia Press (2013). *Personal Data Regulations in Colombia: The New Legal Trend for Companies.* Retrieved from http://www.worldservicesgroup.com/publications.asp?action=article&artid=5572#pdf

Carson, A. (2013). Consent is King in Latin America: Navigating the Eight Existing DPAs with a Look to the Future. *International Association of Privacy Professionals.* Retrieved from https://iapp.org/news/a/2013-06-03-consent-is-king-in-latin-america-navigating-the-eight-existing/

Chirino Sanchez, A. (1997). Las Tecnologías de la Información y el Proceso Penal. *Nexos Costa Rica.* Retrieved from http://www.nexos.co.cr/cesdepu/revelec/penaclarkel/Chirino14.htm

Cornell University Law School (n.d.). *"Habeas Corpus." Legal Information Institute.* Retrieved from https://www.law.cornell.edu/wex/habeas_corpus

Council of Europe (2001). *Convention on Cybercrime*. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=PEmVfagc

Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Retrieved from http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Cruz, X. (2012). Data Protection and Privacy Issues in Latin America. *Cloud Times*. Retrieved from http://cloudtimes.org/2012/11/21/data-protection-privacy-issues-latin-america/

Derechos Digitales (2016). *Internet en México: Derechos humanos en el entorno digital.* Mexico City: Derechos Digitales.

DeVries, W. T. (2003). Protecting Privacy in the Digital Age. *Berkeley Technology Law Journal,*

18 (1), pp. 283-310. Retrieved from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1407&context=btlj

Dunn Cavelty, M. (2014). Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics,* 20 (3), pp. 701-715.

Falcon, E. (1996). *Habeas Data: Concepto y Procedimiento.* Buenos Aires: Abeledo Perrot.

García, C. (2016). Acepta MC que padrón en Amazon pertenece al partido. *El Universal.* Retrieved from http://www.eluniversal.com.mx/articulo/nacion/politica/2016/04/27/acepta-mc-que-padron-electoral-en-amazon-pertenece-al-partido>>

Genderen, R. (2008). *Cybercrime investigation and the protection of personal data and privacy.* CIUDAD: Economic Crime Division, Council of Europe. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study5-d-provisional.pdf

Global Project on Cybercrime (2011). *Cybercrime Strategies.* Economic Crime Division, Council of Europe. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

Gozon, F. E. & Orosa, T. J. (2007). The Sovereign Individual: The Writ of Habeas Data and the Right to Information Privacy. *Ateneo Law Journal* 52, pp. 648-664

Guadamuz, A. (2000). Habeas Data: The Latin-American Response to Data Protection. *Journal of Information, Law, and Technology.* Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz

Gutierrez, H. & Korn, D. (2013). Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America. *University of Miami Inter-American Law Review*, 45 (1). Retrieved from http://repository.law.miami.edu/umair/vol45/iss1/5/

Harding, L. (2016). What are the Panama Papers? A Guide to History's Biggest Data Leak. *The Guardian.* Retrieved from http://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers

Higgott, R. (2005). The Theory and Practice of Global and Regional Governance: Accommodating American Exceptionalism and European Pluralism. *GARNET Working Paper,* 1 (5). Retrieved from http://www2.warwick.ac.uk/fac/soc/pais/research/researchcentres/csgr/garnet/working-papers/0105.pdf

International Telecommunication Union (2016). *ITU Releases ICT 2015 Figures*. Retrieved from http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.V05JvPnhDIU

Kirsh, E., Phillips, D. y D. McIntyre. (1996). Recommendations for the Evolution of Cyberlaw. *Journal of Computer-Mediated Communication* 2 (2).

Laurant, C. (2010). *Recent Cyber-crime Court Decisions from Latin America Legal and Policy Developments*. Retrieved from http://www.slideshare.net/cedriclaurant/cybercrime-court-decisions-from-latin-america-legal-amp-policy-developments-htcia-conference-atlanta-ga-usa-20-sept-2010

Levi, M. & Stoker, L. (2000). Political trust and trustworthiness. *Annual Review of Political Science* 3, pp. 475-507.

Leiva, A. (2013). Data Protection Law in Spain and Latin America: Survey of Legal Approaches. *American Bar Association*. Retrieved from http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html

Litwak, R. S. & King, M. (2015). Cybersecurity treaties may be nice but it's really every country for itself. *Digital Futures Project.* Retrieved from https://www.wilsoncenter.org/article/cybersecurity-treaties-may-be-nice-its-really-every-country-for-itself

Martínez-Herrera, M. (2011). From Habeas Data Action to Omnibus Data Protection: The Latin American Privacy (R)Evolution. *White & Case Technology Newsflash*. Retrieved from http://www.whitecase.com/files/Publication/e5d9876a-bf18-4267-8de7-723c3121e009/Presentation/PublicationAttachment/ab31c92c-c423-4bcb-a7d7-74c822baaa22/article_From_Habeas_Data_Action_to_Omnibus_Data_Protection.pdf

MicroMarket Monitor (2015). *Latin America Cloud Analytics*. Retrieved from http://www.micromarketmonitor.com/information-and-communication-technology-industry-2.html

Morgan, S. (2015). *Multibillion-Dollar Cybersecurity Markets in Asia Pacific and Latin America*. Retrieved from http://sandhill.com/article/multibillion-dollar-cybersecurity-markets-in-asia-pac-and-latin-america/

OAS, Committee on Political and Juridical Affairs (2012). *Comparative Study: Data Protection in the Americas Different existing legal regimes, policies and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation*. Retrieved from http://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12_en.pdf

OAS, Department of International Law 1 (2012). *Data Protection*. Retrieved from http://www.oas.org/dil/data_protection.htm

OAS, Department of International Law 2 (2012*). Relation between Privacy Protection, Data Protection and Habeas Data*. Retrieved from http://www.oas.org/dil/data_protection_privacy_habeas_data.htm

OAS & Trend Micro (2013). *Latin America and the Caribbean Cybersecurity Trends and Government Responses*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Permanent Council of the Organization of American States Committee on Political and Juridical Affairs (2012). *Comparative Study: Data Protection in the Americas*. Washington, D.C.

PwC. (2015). *Cybersecurity in Mexico*. Retrieved from file:///C:/Users/Administrator/Downloads/20150917-kc-cybersecurity.pdf

Raigada, A. T. (2009). Reutilización de información pública y protección de datos personales. *Revista General de Información y Documentación*, pp. 243-264.

Saavedra, B. (2016). Las infraestructuras críticas en América Latina: Conectada, dependiente y vulnerable. *Perry Center Occasional Paper*, pp. 3-21.

Saavedra, B. (2015). Inteligencia Estratégica en un mundo globalizado en Latinoamérica: Retos y desafíos en el siglo XXI*, Revista Policía y Seguridad Pública*, 5 (2), pp. 75-106. Retrieved from http://www.lamjol.info/index.php/RPSP/article/view/2326

Saavedra, B. (2015). Cybersecurity in Latin America and the Caribbean: The state of readiness for the defense of cyberspace. *William J. Perry Center for Hemispheric Defense Studies*, pp. 3-12. Retrieved from http://chds.dodlive.mil/files/2013/12/pub-other-saavedra.pdf

Silva, A. C. (2011). El "Nivel Adecuado de Protección" para las transferencias Internacionales de Datos Personales desde la Unión Europea. *Revista de Derecho (Valparaíso)*, pp. 327-356.

Thomas, B. (2007). *Policy Brief: Habeas Data as a Policy Toward Corporate Data Aggregation.* Retrieved

from http://www.eecs.harvard.edu/cs199r/fp/Brett.pdf

Tschentscher, A. & Lehner, C. (2013). The Latin American Model of Constitutional Jurisdiction: Amparo and Judicial Review. *Social Science Research Network.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2296004

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review* 4 (5). Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Westin, A. (1967). *Privacy and Freedom.* New York: The Bodley Head Ltd.

Legal Documents

Argentina, *National Constitution of the Argentine Republic* (1994). Retrieved on May 5, 2016 from: http://pdba.georgetown.edu/Constitutions/Argentina/argen94_e.html

Brazil, *Constitution of the Federative Republic of Brazil* (1988). Retrieved on April 30, 2016 from: http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html

Colombia, *Ley Estatutaria 1581, "Por el cual se dictan disposiciones generales para la protección de datos personales".* Retrieved on April 30, 2016 from: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf

European Commission (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Retrieved on April 30, 2016 from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles. Retrieved on April 30, 2016 from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

Mexico, *Federal Law on Protection of Personal Data held by Private Parties* (2010). Retrieved on May 21, 2016 from: http://inicio.ifai.org.mx/English/1%20Data%20Protection%20Law.pdf

Paraguay, *Constitution of the Republic of Paraguay* (1992). Retrieved on May 5, 2016 from: http://pdba.georgetown.edu/Constitutions/Paraguay/para1992.html

Peru, *Political Constitution of Peru* (1993). Retrieved on May 5, 2016 from: http://pdba.georgetown.edu/Constitutions/Peru/per93.html

United Kingdom, *Data Protection Act 1998.* Retrieved on May 12, 2016 from: http://www.legislation.gov.uk/ukpga/1998/29/contents